



Trabajo de Fin de Máster

LA PROBLEMÁTICA DE LA INCLUSIÓN DE LA DIGITALIZACIÓN Y LA VIDEOVIGILANCIA EN EL ÁMBITO LABORAL.

Presentado por:

Natalia Badenas Ros

Tutor/a:

Inmaculada Ballester Pastor

Máster Universitario en Abogacía

Curso académico 2019/20
Fecha de defensa: Enero 2020

Resumen

Las nuevas tecnologías han tenido una enorme injerencia en el ámbito de las relaciones laborales, y más concretamente en lo que concierne al control empresarial. Esta digitalización social exige una constante adaptación de nuestra normativa nacional a las nuevas situaciones y controversias originadas en materia de videovigilancia y protección de datos, siempre en garantía de los derechos fundamentales reconocidos a las partes intervinientes de una relación laboral, estos son, trabajador y empresario, sin que en ningún caso la utilización de estos medios digitales de fiscalización laboral puedan menoscabar las garantías que tradicionalmente nuestra Constitución ha reconocido al trabajador.

Palabras clave

Derecho a la intimidad, derecho a la protección de datos personales, cámaras de videovigilancia, ámbito laboral, derechos fundamentales, garantías constitucionales, nuevas tecnologías, control empresarial, deber informativo, prueba.

ANEXO ABREVIATURAS

ART: Artículo.

AEPD: Agencia Estatal de Protección de Datos.

CE: Constitución de 1978.

ET: Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LODD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LRJS: Ley 36/ 2011, de 10 de octubre, reguladora de la jurisdicción social.

LEC: Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

STSJ: Sentencia del Tribunal Superior de Justicia.

STS: Sentencia del Tribunal Supremo.

STC: Sentencia del Tribunal Constitucional.

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos.

TSJ: Tribunal Superior de Justicia.

TS: Tribunal Supremo.

TC: Tribunal Constitucional.

TEDH: Tribunal Europeo de Derechos Humanos.

ÍNDICE

1. Introducción	p. 1
2. Evolución de la doctrina judicial actual	pp. 2 - 12
2.1.La doctrina marco sobre el derecho a la intimidad en materia de videovigilancia en el ámbito laboral: SSTC 98/2000, de 10 de abril (Asunto Casino de la Toja) y 186/2000, de 10 de julio (Asunto Ensidesa).....	p. 2
2.2.La introducción del derecho a la protección de datos y la nueva doctrina sobre las cámaras de videovigilancia de carácter fijo: STC 29/2013, de 11 de marzo (Asunto Universidad de Sevilla).....	p. 5
2.3.Vuelta a la doctrina inicial: STC 39/2016, de 3 de marzo (Asunto Bershka).....	p. 7
2.4.El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores: la STEDH de 9 de enero 2018 (Asunto López Ribalta y otros contra España).....	p. 9
3. Relevancia de los derechos fundamentales implicados.....	pp. 12 - 15
3.1 Incidencia de las nuevas tecnologías en los derechos fundamentales.....	p. 12
3.2 Contraposición de intereses constitucionales: el derecho a la libertad de empresa vs. el derecho a la intimidad de los trabajadores.....	p. 13
4. Evolución de la normativa de protección de datos y especial mención a la nueva Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales	pp. 15 - 21

4.1 Precedentes normativos.....	p. 15
4.2 Principales novedades de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	p. 17
5. El dato personal convertido en prueba: validez de las imágenes obtenidas a través de sistemas de videovigilancia como prueba en el proceso.....	pp. 22 - 28
5.1.Cuestiones procesales controvertidas en torno a la prueba obtenida a través de cámaras de videovigilación.....	p. 22
5.1.1.Naturaleza y fuerza probatoria.....	p. 22
5.1.2.Aportación al proceso laboral.....	p. 24
6. Conclusiones.....	pp. 29 - 30
7. Bibliografía	pp. 31 - 32
8. Legislación	p. 33
9. Anexo jurisprudencial	pp. 34 - 45

1. INTRODUCCIÓN.

El presente trabajo tiene como objeto principal abordar un derecho tan fundamental como es el de la protección de datos, derecho que, aunque desconocido para muchos, cobra cada día mayor protagonismo en una sociedad que navega hacia una Revolución digital que será clave en nuestro día a día.

La entrada de este derecho en el ámbito laboral no iba a tardar en producirse. Prueba de ello es que en la actualidad la mayoría de las empresas tienen incorporados en sus centros de trabajo novedosos dispositivos electrónicos capaces de ocuparse de funciones tales como el control de la actividad laboral de los trabajadores y lo hacen a través de cámaras de videovigilancia.

La implantación de estos dispositivos de grabación de imágenes en los lugares de trabajo ha cobrado un gran protagonismo en los últimos años - tanto a nivel normativo como jurisprudencial -, por lo que he considerado relevante dirigir la atención de este estudio, en su primera parte, a analizar y estudiar las distintas sentencias que, en su mayor parte, el Tribunal Constitucional, ha tenido ocasión de pronunciar, resoluciones éstas que constituyen la doctrina judicial clave acerca de la validez del uso de la videovigilancia en los centros de trabajo por parte de las empresas.

La segunda parte del trabajo se dedica a tratar la incidencia que estos sistemas de videovigilancia tienen sobre los derechos fundamentales así como a abordar las principales novedades introducidas por la reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por último, he considerado oportuno concluir el estudio abordando una cuestión de carácter procesal: si la prueba adquirida a través de imágenes obtenidas por sistemas de videovigilancia es válida en primera instancia y si, asimismo, ésta puede ser revisada en el recurso de suplicación.

2. EVOLUCIÓN DE LA DOCTRINA JUDICIAL ACTUAL.

Dada la escasa regulación normativa existente sobre el uso de las cámaras en el ámbito de las relaciones laborales resulta imprescindible acudir a las resoluciones judiciales que, desde hace décadas, vienen pronunciándose al respecto siempre en aras a determinar cuáles son las situaciones en las que pueden utilizarse, con qué fines y límites.

A *grosso modo* existen cuatro importantes pronunciamientos emitidos por nuestro TC en materia de videovigilancia que merecen una exposición pormenorizada.

2.1 La doctrina marco sobre el derecho a la intimidad en materia de videovigilancia en el ámbito laboral: SSTC 98/2000, de 10 de abril (Asunto Casino de la Roja)¹ y 186/2000, de 10 de julio (Asunto Ensidesa)².

La primera de las mentadas sentencias recoge un supuesto de hecho que cabe advertir, no versa sobre la debida utilización o no de las cámaras de videovigilancia en el lugar del trabajo, sino sobre la decisión de la empresa de instalar unos micrófonos (que permitían recoger y grabar las conversaciones del lugar dónde se colocaban) junto a un sistema de circuito cerrado de televisión del que ya disponía el casino desde su apertura. Pese a no circunscribirse al ámbito de la videovigilancia, he considerado interesante traerla a colación por cuanto es una de las primeras sentencias dictadas por nuestro TC en las que se discute si un medio de vigilancia y control empresarial supone una intromisión o no en la intimidad de los trabajadores.

De manera sucinta, el TC dictaminó que en el caso enjuiciado la medida de instalar micrófonos en algunos puntos concretos del casino no había respetado los principios de proporcionalidad e intervención mínima que rigen en todo caso

¹ Rec. 4015/1996.

² Rec. 2662/1997.

la modulación de los derechos fundamentales, siendo que la única finalidad de la empresa era *“dar un plus de seguridad ante eventuales reclamaciones de los clientes”* por lo que la medida resultaba totalmente desproporcionada para el sacrificio que implicaba del derecho a la intimidad de los trabajadores. Además, consideró que dicha finalidad buscada por la empresa ya se veía satisfecha a través del sistema de seguridad de circuito cerrado de televisión con el que ya contaba el casino desde su apertura. Por último, recalcó la inexistencia de sospecha alguna o detección de quiebra en los sistemas de control existentes que pudiese haber justificado en cierta medida tal decisión.

El segundo de estos pronunciamientos, la STC 186/2000 de 10 de julio, en cambio, sí versa sobre un supuesto de implantación de cámaras de videovigilancia en el centro de trabajo por lo que merece un estudio más detallado.

La sentencia trae a colación un supuesto que versa sobre la instalación de un circuito cerrado de televisión en un economato, medida que decide implantar la empresa con la finalidad de controlar la zona de caja tras haberse percatado de la existencia de graves irregularidades en uno de los puestos de trabajos a la vista de un llamativo descuadre. Las cámaras revelaron cómo uno de los trabajadores había realizado maniobras fraudulentas en el cobro de productos de manera repetida sustrayendo determinadas cantidades de la caja, motivo por el que la empresa decidió despedirlo. Tras haber agotado el trabajador la vía judicial social sin éxito³, éste solicitó posteriormente el amparo al TC por entender que ese tipo de control laboral había conculcado su derecho a la

³ El Juzgado de lo Social concluyó que la prueba exhibida de las cintas de vídeo era ajustada a Derecho por cuanto *“se plantea a partir de una situación de sospecha fundada, que el medio utilizado se presenta como el único viable (...) que, además, se empleó con los límites mínimos, ya que se concretó a la vigilancia de un puesto de trabajo que es eminentemente público, donde el trabajador está a la vista de todo el mundo y en el que es improbable que se registre acto alguno que entre en la esfera de su intimidad personal (...).”*

Tras ser desestimada su pretensión, el trabajador recurrió en suplicación sin obtener éxito tampoco en esta vía al declararse que: *“las cintas de vídeo no son, por sí mismas un medio de prueba ilegítima (...), la intimidad del trabajador no resulta agredida por el solo hecho de ser objeto de filmaciones (...), la materia objeto de filmación no va referida a su vida íntima sino a obtener un conocimiento de cuál es su comportamiento laboral (...), la instalación de una cámara fija sobre la caja registradora y el mostrador de mercancías es un sistema de control de trabajo, una labor de vigilancia que corresponde a la empresa y a la que autoriza el art.20 del ET”*.

intimidad personal y a la propia imagen consagrado en el artículo 18.1 de la Constitución Española. El TC, no obstante, desestimó su petición al considerar que la instalación de las cámaras se había llevado a cabo de manera lícita sin producir intromisión alguna en la intimidad del recurrente pues era una medida justificada al existir una previa, razonada y fundada sospecha sobre la comisión de una conducta ilícita por parte del recurrente y, además, superaba el triple juicio de proporcionalidad ya que era *idónea* para la finalidad buscada por la empresa (que era la de acreditar si el trabajador efectivamente llevaba a cabo la conducta sospechada o si por el contrario se trataba de una mera confusión); *necesaria* al poder servir de prueba para dilucidar la cuestión y *equilibrada*, pues las cámaras instaladas sólo enfocaron la zona estrictamente necesaria para comprobar la sospechada conducta del trabajador (zona de la caja) y durante el mínimo tiempo requerido para ello.

Por tanto, hasta ese momento, la instalación de cámaras *ad hoc* en los centros de trabajo estaba permitida siempre que la empresa justificase la adopción de tal medida en una fundada y razonable sospecha⁴ de la comisión de una conducta ilícita por parte de uno o varios de sus trabajadores y siempre y cuando la medida superase el triple juicio de proporcionalidad⁵, esto es, que la misma fuese idónea, necesaria y equilibrada para el fin buscado por la empresa. En caso de no respetar dichas directrices, la medida de control laboral se consideraba vulneradora del derecho a la intimidad de los trabajadores.

Este criterio también se extendió para el caso de cámaras fijas o permanentes ya instaladas en la empresa, si bien respecto de las mismas no se suscitaba tanta problemática siempre - claro está - que las mismas estuvieran

⁴ En el caso enjuiciado, el TC consideró que no era necesario informar al Comité de Empresa y mucho menos al trabajador, pues hacerlo frustraría el objetivo en sí de la medida, cual era el de acreditar si el trabajador cometía efectivamente las irregularidades sospechadas.

⁵ Vid. STC 186/2000 de 10 de julio, rec. 2662/1997 FJ 6º: *"Dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, la modulación de los mismos sólo deberá producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador, y muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE, teniendo siempre presente el principio de proporcionalidad"*.

debidamente señalizadas con sus correspondientes carteles de manera que los trabajadores pudiesen conocer su existencia.

2.2 La introducción del derecho a la protección de datos y la nueva doctrina sobre las cámaras de videovigilancia de carácter fijo. STC 29/2013, de 11 de febrero (Asunto Universidad de Sevilla)⁶.

Tras quedar fijado el *modus operandi* que debía regir la instalación de sistemas de videovigilancia en el ámbito laboral, el TC dio un giro doctrinal en el año 2013 tras resolver un asunto que tuvo por objeto la incoación de un expediente disciplinario de un trabajador de la Universidad de Sevilla, al haber constatado el centro universitario que éste incumplía su jornada laboral, conducta que había quedado acreditada mediante la grabación de imágenes de una de las cámaras de seguridad existentes en el recinto, cámaras que se encontraban instaladas a los efectos de controlar el acceso a sus campus y centros (concretamente una de ellas enfocaba el acceso directo del despacho del trabajador recurrente). Debemos anticipar que la Universidad disponía de la autorización administrativa concedida por la Agencia Estatal de Protección de Datos, que, además, ésta había advertido de la existencia de las cámaras colocando los oportunos carteles informativos y que, sobre el trabajador en cuestión, existían fundadas sospechas sobre el incumplimiento de su horario laboral. Pues bien, tras haber sido expedientado por los hechos descritos, el trabajador interpuso demanda por entender que la utilización que se había hecho de las citadas imágenes había vulnerado su derecho a la protección de datos de carácter personal consagrado en el art. 18.4 CE ya que en ningún momento se le había informado de manera previa, clara y expresa de los fines a los que se podían destinar tales imágenes (entre los cuales se encontraba el de supervisar su actividad laboral).

El TC otorgó el amparo solicitado entendiendo que la Universidad debía haber informado previamente al trabajador de los fines de control laboral a los que podían destinarse las imágenes captadas por las cámaras de seguridad instaladas en el campus. Por tanto, este pronunciamiento constitucional

⁶ Rec.10522-2009.

constituyó un antes y un después en materia de videovigilancia en el ámbito laboral⁷: ya no era suficiente el distintivo informativo⁸ debidamente colocado por la empresa en aquellas zonas en las que existieran cámaras de videovigilancia, ni tampoco la mera justificación por parte de la empresa de una previa, fundada y razonable sospecha sobre la conducta ilícita de uno o varios trabajadores de la empresa, como tampoco que la medida superase el triple juicio de proporcionalidad; ahora, se requería junto al cumplimiento de los anteriores requisitos, también que el empleador hubiera informado de manera previa y expresa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida.

En el caso enjuiciado el TC no entró siquiera a valorar si la medida adoptada había superado el triple juicio de proporcionalidad, pues el hecho de no haber informado al trabajador ya suponía que la conducta de la Universidad (consistente en utilizar las grabaciones de imágenes para controlar el cumplimiento de la jornada laboral del trabajador) era contraria al contenido del art. 18.4 CE. A tal consideración llegó tras haber manifestado que la grabación de imágenes constituía un <<dato de carácter personal>> y que el derecho a la información previa⁹ constituía el núcleo esencial de este derecho fundamental, razón por la que de no cumplirse el deber de información previa resultaba ya innecesario aplicar el tradicional examen de proporcionalidad pues la conducta empresarial devenía ilegítima.

Así las cosas, la doctrina judicial existente en este tema en el periodo de tiempo comprendido entre la STC 186/2000 de 10 de julio y la STC 29/2013, de 11 de febrero variaba en atención al carácter fijo o *ad hoc* de las cámaras de

⁷ La STC 29/2013, de 11 de febrero, rec. 10522/2009 dio origen a una nueva doctrina que sujetaba el ejercicio de las facultades del empresario al cumplimiento del deber de información previa a los trabajadores acerca del contenido y objetivo específicos de la correspondiente medida de vigilancia y control.

⁸ Distintivo informativo exigido en virtud del artículo 3a) de la Instrucción 1/2006, de 8 de noviembre, de la AEPD sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras.

⁹ Vid. STC 29/2013, de 11 de febrero, rec. 10522/2009, en la que se recoge la definición de derecho a la información previa como *"derecho que tiene todo aquél afectado por este tipo de sistemas de videovigilancia, y que se concreta en el derecho a saber quién posee los datos recogidos por dichas imágenes y con qué fin son almacenados"*.

videovigilancia. Para aquellos supuestos en los que las imágenes habían sido obtenidas mediante cámaras instaladas *ad hoc*, debía seguirse el procedimiento asentado por la STC 186/2000 de 10 de julio (que exigía como requisitos indispensables para la licitud de la medida: la existencia de una previa, fundada y razonable sospecha sobre la conducta ilícita de algún trabajador y la superación del examen o juicio de proporcionalidad). Por el contrario, si las imágenes se habían obtenido a través de cámaras de vigilancia fijas, el criterio a seguir era el fijado por la STC 29/2013 de 11 de febrero, que supeditaba la legitimidad de la medida a la previa información por parte del empleador sobre los fines laborales concretos a los que se podían destinar las imágenes captadas, resultando insuficiente el cumplimiento del oportuno distintivo informativo y la superación del triple juicio de proporcionalidad.

2.3 Vuelta a la doctrina inicial: la STC 39/2016 de 3 de marzo (Asunto Bershka)¹⁰.

La mentada sentencia anuló después el criterio que había sido fijado por la STC 29/2013, de 11 de febrero¹¹ dejando a un lado el deber de información previa que se venía exigiendo a las empresas como requisito indispensable para el tratamiento de sistemas de videovigilancia con fines de control laboral. El supuesto de hecho que dio origen a este nuevo *modus operandi* giraba en torno al despido de una trabajadora de una tienda de ropa. Lo que ocurrió fue que, la empresa, tras percatarse de diversas irregularidades en la caja donde la misma desempeñaba su actividad, decidió instalar cámaras de videovigilancia con el fin de acreditar si se trataba de una mera confusión o de una verdadera conducta ilícita, para en este último caso, proceder a adoptar las medidas pertinentes. La empresa colocó en el escaparate el oportuno distintivo informativo, pero no comunicó de manera previa y expresa a los trabajadores la instalación de la cámara. Las imágenes obtenidas por medio de las cámaras de videovigilancia revelaron la conducta ilícita de la trabajadora (consistente en

¹⁰ Rec. 7222/2013.

¹¹ Criterio consistente en supeditar la licitud de la medida de fiscalización laboral (mediante sistemas de videovigilancia) a la obligación del empleador de informar de manera previa y expresa, clara e inequívoca a los trabajadores de las finalidades concretas a las que podían destinarse las imágenes obtenidas por medio de esos sistemas digitales.

apropiarse dinero de la caja de la tienda de manera reiterada), por lo que la empresa procedió a despedirla. La trabajadora acudió entonces, a la vía judicial solicitando la nulidad del despido por entender que el mismo atentaba contra su honor, intimidad y dignidad, pues consideraba que, en casos como el suyo, se exigía ineludiblemente la información previa al trabajador, requisito que la empresa había incumplido (criterio que había instaurado la STC 29/2013, de 11 de febrero y al que se acogió la actora).

Tras ser desestimadas sus pretensiones en primera y segunda instancia¹², la trabajadora solicitó posteriormente el amparo ante el TC, órgano jurisdiccional que denegó tal amparo al considerar que, en el caso enjuiciado la empresa no tenía la obligación de recabar el consentimiento expreso de la trabajadora para el susodicho tratamiento de las imágenes obtenidas a través de las cámaras instaladas en la tienda con la finalidad de controlar la actividad laboral de los trabajadores, pues la decisión de instalar dichas cámaras constituía una medida empresarial permitida por el art. 20.3 del Estatuto de los Trabajadores, motivo por el que el consentimiento se entendía implícito en la propia aceptación del contrato. Además, el TC incidió en que la empresa también había cumplido con la obligación de colocar el distintivo informativo exigido legalmente requisito que, a su vez, implicaba el cumplimiento del deber de información contenido en el art. 5 de la entonces vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Es decir, en ese momento, el deber de información previa se entendía cumplido con la mera colocación del distintivo informativo en la zona en la que se encontraran las cámaras de videovigilancia sin ser necesario el deber de informar a los trabajadores de manera previa y expresa sobre la existencia y finalidad de la

¹² El Juzgado de lo Social declaró procedente el despido al entender que la empresa había cumplido escrupulosamente la normativa relativa a la protección de datos aplicable al caso concreto (téngase en cuenta que en ese momento la Ley aplicable era la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por lo que la decisión del Tribunal tuvo en consideración el contenido de la misma - a destacar el art. 5 que recogía *“el derecho de información en la recogida de datos”*). Posteriormente, el trabajador interpuso recurso de suplicación, el cual fue igualmente desestimado por el TSJ de Castilla y León al entender que *“la decisión empresarial de colocar una cámara de videovigilancia satisfizo el juicio de proporcionalidad constitucionalmente exigido para poder afirmar su legalidad y legitimidad”* y que *“la referida medida debe considerarse idónea, necesaria y proporcional”* por lo que la medida superaba el triple juicio de proporcionalidad.

medida de fiscalización laboral. Ahora bien, lo que realmente debía ponderarse era si la finalidad a la que la empresa destinaba dichas imágenes efectivamente comprendía la de controlar la relación laboral ya que, de destinarse a una finalidad ajena a ésta, el empresario quedaba en todo caso obligado a solicitar el consentimiento expreso de los trabajadores, no resultando suficiente la colocación del distintivo informativo al que se refiere la mentada Instrucción.

Este giro doctrinal - que no hizo más que reivindicar el criterio asentado por la precedente STC 186/2000, de 10 de julio - en ningún caso quiso significar la eliminación de una tan merecida protección del derecho a la intimidad y a la protección de datos de carácter personal, pues en la misma medida se seguía exigiendo que la medida de control empresarial resultase justificada por existir una previa, fundada y razonada sospecha y una adecuación de la misma al examen de proporcionalidad.

2.4 El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores: la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero 2018, asuntos núms. 1874/13 y 8567/13 (Asunto López Ribalta y otros contra España).

Si hay alguna sentencia que merece especial atención en materia de videovigilancia en el ámbito laboral ésta es, sin duda, la dictada por el Tribunal Europeo de Derechos Humanos el pasado 9 de enero de 2018¹³.

El supuesto de hecho en cuestión es muy similar a otros anteriores que han visto nuestros tribunales (y que ya hemos tenido ocasión de comentar). Concretamente versa sobre una empresa de supermercados que, ante las sospechas de irregularidades entre los niveles de stock del supermercado y lo realmente vendido, decide instalar unas cámaras de videovigilancia (unas

¹³ Vid. STEDH de 9 de enero de 2018, pronunciamiento considerado por muchos, como una llamada de atención por parte del TEDH a nuestros Tribunales, en especial, por cuanto respecta a la videovigilancia oculta (también denominada *ad hoc*).

visibles y otras ocultas)¹⁴ con el fin de acreditar las sospechas de la existencia de conductas generadoras de tales irregularidades. La instalación de las cámaras visibles fue puesta en conocimiento tanto de los trabajadores como del Comité de empresa con carácter previo; sin embargo, de la instalación de las cámaras *ad hoc* no se informó de manera alguna ni a los trabajadores, ni al Comité, pues la empresa entendió que hacerlo frustraría la finalidad buscada, que no era otra que la de averiguar la razón del descuadre de stock.

Pues bien, las cámaras pudieron constatar la conducta inapropiada que se sospechaba gracias a que las imágenes revelaron cómo varios trabajadores del supermercado no sólo habían hurtado determinados productos, sino que habían cooperado también en hurtos efectuados por parte de los propios clientes. A la vista de tales pruebas, la empresa decidió despedir a los trabajadores implicados por transgresión de la buena fe contractual y abuso de confianza (art. 54.2 ET).

Los tribunales nacionales estimaron que la medida empresarial había resultado justificada por las previas y razonables sospechas existentes, además, consideraron que se trataba de una medida idónea, necesaria y proporcionada por cuanto no existía otra manera de poder acreditar la sospechada conducta ilícita de los trabajadores. Llegados a este punto, cabe hacer un inciso para recordar que la jurisprudencia española en el momento de los hechos enjuiciados venía exigiendo, con carácter general, que la decisión de instalar sistemas de videovigilancia - cámaras fijas - en el ámbito laboral fuese puesta en conocimiento de los trabajadores con carácter previo y de manera expresa, de modo que los afectados pudiesen conocer la finalidad concreta de la medida en cuestión. En caso de tratarse de cámaras ocultas se exigía la existencia de una finalidad legítima para considerar la medida lícita, entendiendo por <<finalidad legítima>> la existencia de una fundada y razonable sospecha por

¹⁴ Vid. STEDH de 9 de enero de 2018, entre cuyos hechos se relata que *"tal y como se informó, las primeras se instalaron con la finalidad de captar posibles hurtos de clientes y fueron colocadas de tal manera que enfocaban las entradas y salidas del supermercado; las segundas, por el contrario, se implantaron con la finalidad de grabar y controlar posibles hurtos de empleados, enfocando el área de los cajeros"*.

parte de la empresa de la comisión de un ilícito por parte de uno o varios trabajadores.

Es más tarde cuando el mentado asunto llegó al Tribunal de Estrasburgo, órgano judicial que, tras un pormenorizado análisis y estudio de los hechos y las circunstancias concurrentes manifestó su discrepancia¹⁵ abriendo un nuevo horizonte a la evolución de la doctrina judicial existente en materia de videovigilancia encubierta o *ad hoc*, al manifestar que ese tipo de fiscalización empresarial hacia un trabajador en su lugar de trabajo debía ser apreciada como *“una considerable intromisión en su vida privada”*¹⁶, considerando indispensable, en estos casos, que el empleador informara previamente, de manera clara y precisa a los trabajadores de la existencia y finalidad de la medida aún cuando la videovigilancia fuese encubierta, pues la existencia de una fundada y razonable sospecha no agotaba la licitud de la medida empresarial.

En resumidas cuentas, el TEDH a través de la citada sentencia hace una advertencia a los tribunales nacionales poniendo en el punto de mira el deber de información de los datos personales, deber que considera inserto en la legislación española de protección de datos (en aquél momento, la normativa aplicable era la LOPD)¹⁷, motivo por el que entiende que los tribunales nacionales deben basar sus pronunciamientos en una rigurosa exigencia de este deber (se trate de videovigilancia fija o permanente o *ad hoc*); además el Tribunal recuerda que este derecho al mantenimiento por parte de las

¹⁵ Vid. STEDH, de 9 de enero de 2018 FJ 69º: *“Este Tribunal no puede compartir la visión de los tribunales nacionales sobre la proporcionalidad de las medidas adoptadas por el empleador (...). La videovigilancia llevada a cabo por el empleador, teniendo lugar durante un tiempo prolongado, no cumple con las exigencias del art. 5 - de la entonces vigente LOPD -, y en particular con la obligación de informar sobre todo lo concerniente a la existencia y particulares características del sistema de recogida de datos personales”*.

¹⁶ Sobre esta materia, Vid. GONZÁLEZ GONZÁLEZ C., “Control empresarial de la actividad laboral mediante la videovigilancia y colisión de los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”, Revista Aranzadi Digital, nº 1, 2018, p. 14.

¹⁷ Art. 5 LOPDCP: *“Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco (...)”*.

empresas de los datos personales de los trabajadores es un derecho fundamental consagrado en nuestra Constitución Española¹⁸.

3. RELEVANCIA DE LOS DERECHOS FUNDAMENTALES IMPLICADOS.

3.1 Incidencia de las nuevas tecnologías en los derechos fundamentales.

El avance tecnológico que experimenta nuestra sociedad precisa de una constante actualización normativa, tendente a garantizar que las nuevas situaciones y contextos en los que los ciudadanos pueden ver involucrados sus derechos, queden cubiertas por nuestras normas. Y es que, dicho avance tecnológico, como veremos a lo largo del trabajo, lleva consigo la evolución de los métodos de control empresarial.

La videovigilancia en el ámbito laboral como método de control empresarial, desde siempre, ha sido una cuestión compleja de tratar, pues la decisión de emplear modernos sistemas de fiscalización del cumplimiento de la prestación laboral por parte del empleador que pretende evidenciar un comportamiento irregular del trabajador choca frontalmente con determinados derechos fundamentales de éste último.

Pues bien, pese a haber considerado que esta cuestión ya estaba superada, en los últimos años la implantación de sistemas de videovigilancia a través de cámaras de video, ya sean estas permanentes (fijas) o ad hoc (temporales u ocultas), ha exigido una mayor precisión e interpretación por parte de los tribunales, que frente a determinadas lagunas normativas, han debido abrir camino para resolver las nuevas problemáticas suscitadas en materia de videovigilancia en el ámbito laboral. Así pues, el debate sobre el uso de las cámaras de videovigilancia como medida empresarial para sancionar conductas de los trabajadores, sigue estando en el punto de mira.

¹⁸ Art. 18.4 CE: *“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.

Este método de control empresarial está reconocido implícitamente dentro de las facultades de organización y control empresarial del artículo 20.3 del ET¹⁹, pero no debe obviarse tampoco su tradicional liza con otros derechos que deben garantizarse del mismo modo a los trabajadores y considerados también como fundamentales, como lo son el derecho a la intimidad y el derecho a la protección de datos de carácter personal, reconocidos en los artículos 18.1 y 18.3 de la CE²⁰. Ello exigirá en todo momento un uso correcto y de absoluto respeto a todos esos derechos fundamentales, debiendo garantizarse el equilibrio entre el derecho a la libertad de empresa y los derechos fundamentales de los trabajadores en el desarrollo de la relación de trabajo.

3.2 Contraposición de intereses constitucionales: el derecho a la libertad de empresa vs. el derecho a la intimidad de los trabajadores.

El uso de la videovigilancia en el ámbito laboral provoca pues, la entrada en juego de ambos derechos fundamentales ya que la utilización que pueda hacer el empleador de dicho método de control afecta directamente a la esfera más íntima de los trabajadores pues la misma puede vulnerar sus derechos. De ahí la importancia de que, la decisión de implantar cámaras de videovigilancia en un lugar de trabajo, deba siempre salvaguardar en todo momento la esfera privada de los trabajadores.

Sin embargo, la salvaguarda de tal <<intimidad>>, nunca ha sido cuestión sencilla en la práctica pues la norma jurídico-laboral no siempre ha establecido una regulación específica y concreta sobre este asunto, lo que ha llevado, como ya se ha dicho, a que nuestros tribunales hayan debido pronunciarse al respecto de manera reiterada. En el seno de esa labor interpretativa los

¹⁹ Artículo 20.3 ET: *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”*.

²⁰ Artículos 18.1 CE: *“se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”* y 18.4 CE: *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.

tribunales han velado siempre por garantizar que la adopción de las medidas de videovigilancia se realicen en absoluto respeto del derecho fundamental a la intimidad de las personas afectadas delimitando, en la medida de lo posible los supuestos en los que el control de videovigilancia tiene cabida y en los que no, así como reconociendo cuándo se ha llevado a cabo de manera lícita y cuando no.

Como comentábamos, pese a considerar que la implantación de sistemas de videovigilancia en los lugares de trabajo y sus problemas inherentes habían sido mayoritariamente resueltos resulta que, últimamente la controversia suscitada respecto a esta medida de control empresarial vuelve a estar en el punto de mira. Prueba de ello es que podemos comprobar hoy cómo, en un breve periodo de tiempo, los pronunciamientos de los tribunales se han distanciado y aproximado en mayor o menor medida de la clásica doctrina jurisprudencial que sobre esta materia se ha venido consolidando. La doctrina judicial actual, como veremos pese a no haber seguido el mismo hilo interpretativo en todas las ocasiones, ha contribuido a perfilar, con mayor precisión, el derecho a la protección de datos²¹, convirtiéndolo en un derecho autónomo e independiente, tal y como queda recogido en la tan reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por último, resulta interesante traer a colación otros derechos fundamentales que si bien no reciben el mismo protagonismo que el ya citado derecho a la intimidad personal (al menos por cuánto respecta a la implantación de sistemas de videovigilancia en el ámbito laboral) sí requieren en la misma medida, de una salvaguarda y protección en el ámbito de las relaciones laborales ya que un uso inadecuado de estos dispositivos digitales, a la postre, puede no sólo

²¹ Vid. STC 292/2000, de 30 de noviembre, rec. 1463/2000, en la que se manifiesta que: *"el derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización y omisión de determinados comportamientos"*. Asimismo, continúa diciendo que: *"la función del derecho a la protección de datos es la de garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*.

conculcar la intimidad de las personas, sino también en un momento posterior, otros derechos fundamentales como son el derecho a la tutela judicial efectiva, el derecho a un proceso con todas las garantías así como el derecho a la presunción de inocencia, derechos todos ellos consagrados en el artículo 24 de la CE²².

4. EVOLUCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS Y ESPECIAL MENCIÓN A LA NUEVA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

4.1 Precedentes normativos.

Teniendo presente que, en la actualidad, las relaciones sociales se asientan mayoritariamente en el intercambio de datos personales y que así sucede también, en las relaciones laborales resulta primordial conocer la normativa²³ que, desde hace décadas, se ha ocupado de regular esta materia.

En primer lugar, cabe citar como pionera (por marcar un antes y un después en nuestro país, al haber sido la primera norma en materia de protección de datos aprobada), la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en adelante

²² Artículo 24 CE: *“Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión (...) Asimismo, todos tienen derecho (...) a un proceso público sin dilaciones indebidas y con todas las garantías”*.

²³ Con carácter previo y sin restar protagonismo a la normativa que al presente interesa, debemos hacer referencia a tres importantes declaraciones internacionales en las que se ha reconocido el derecho a la intimidad y a la protección de datos de carácter personal. La primera de ellas, se refiere a la Declaración Universal de Derechos Humanos, en cuyo artículo 12 se dispone que: *“nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”*. En segundo lugar, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa, que en su artículo octavo prevé que: *“toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”*. Por último, el Convenio 108 del Consejo de Europa, establece en su apartado primero que *“se garantizará a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona”*.

“LORTAD”)²⁴, regulación que en su momento, trató de desarrollar lo recogido en el art. 18 de la CE, instaurando, por primera vez, la limitación del uso de la informática para garantizar la intimidad personal.

Con posterioridad, la LORTAD fue derogada por la LOPD²⁵, Ley que en su día adaptó nuestra legislación nacional a la Directiva europea 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos. La misma supuso un desarrollo de la protección de datos mas allá de los datos informatizados, incluyendo, por primera vez, los datos de carácter personal registrados en soporte físico dentro de su ámbito de aplicación.

Finalmente, el último hito en esta evolución ha tenido lugar con la reciente aprobación de la LODD que deroga la anterior LOPD y cuyo estudio resulta fundamental en materia de videovigilancia en el ámbito laboral²⁶. Pues bien, conviene analizar con detalle la incidencia que la misma ha tenido en el ámbito de las relaciones de trabajo, así como cuáles han sido sus principales modificaciones y novedades para con respecto a la normativa anterior²⁷.

²⁴ Vid. Exposición de Motivos de la LORTAD: *“Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor; una frontera que sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley”*.

²⁵ La LOPD constituyó un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

²⁶ A lo largo de sus numerosas disposiciones adicionales y finales, la LODD deja vigente la regulación que sobre la protección de datos personales se recoge en otras disposiciones sectoriales o específicas y procede a la modificación de diversos textos legales afectados por esta nueva normativa, entre ellos el Estatuto de los Trabajadores.

²⁷ Sobre esta materia, Vid. GARCÍA MURCIA, J. y RODRÍGEZ CARDO, I.A, “La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo”, Revista Española de Derecho del Trabajo, nº 216, 2019, pp. 12 y ss.

4.2 Principales novedades de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Desde una perspectiva general la nueva LODD, ha supuesto, para cualquier ciudadano, el reconocimiento de un mayor número de garantías en protección de datos personales, debiendo entender por <<datos personales>> aquellos que comprenden cualquier información relativa a una persona física, viva identificada o identificable²⁸, es decir, las distintas informaciones que, recopiladas, pueden llevar a la identificación de una determinada persona.

Pues bien, adentrándonos en el contenido concreto de esta LODD, conviene diferenciar dos partes dentro de la misma: la primera, en la que (aunque con carácter general) no se detectan grandes novedades, aparecen algunos preceptos que revisten especial interés desde el punto de vista del ámbito de las relaciones de trabajo. En concreto, nos referimos el art. 22, que se encarga de regular el tratamiento de datos personales <<con fines de videovigilancia>> o a partir de sistemas de grabación de sonidos. Pese a no poder considerarlo en su totalidad un precepto de carácter laboral su apartado octavo realiza una mención explícita al tratamiento que el empleador debe realizar respecto de los datos obtenidos mediante sistemas de cámaras o videocámaras y lo hace, redirigiéndole al art. 89²⁹ del mismo cuerpo legal. Asimismo, el citado precepto, se encarga de regular el deber de información que asiste al empleador, un deber que, en la mayoría de ocasiones, ha constituido el punto de controversia en materia de implantación de sistemas de videovigilancia en el ámbito laboral. Ello se ha debido a un constante cambio por parte de la jurisprudencia, que como ya hemos tenido ocasión de analizar, en determinados casos ha considerado que el cumplimiento del deber se agotaba con la mera colocación

²⁸ Art. 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

²⁹ Artículo 89 de la LODD: *“Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (...)”*.

de un distintivo informativo³⁰, y sin embargo en otros casos exigía, además, que el empleador hubiera informado de una manera “expresa, clara y concisa”, a los trabajadores de los fines concretos de la medida adoptada³¹. En los próximos epígrafes, abordaremos con mayor profundidad la cuestión del <<deber informativo>>, analizando las distintas sentencias que se han pronunciado al respecto.

Ahora bien, como decíamos, la primera parte de la LODD no introduce grandes novedades ni cambios (al menos desde el punto de vista laboral), pero sí lo hace en mayor medida su segunda parte. De hecho, en la misma se incluye una regulación especial, circunscrita al ámbito de la empresa y de la relación de trabajo³².

Antes de adentrarnos en el contenido de estos preceptos, resulta conveniente manifestar que, respecto de esta segunda parte, la voluntad del legislador ha sido la de dotar de mayores garantías a los trabajadores, concretamente en una serie de supuestos que, bajo su punto de vista, y precisamente debido a la utilización de medios electrónicos (entre los que se encuentran, las cámaras de videovigilancia), pueden ponerse en riesgo determinados derechos fundamentales de los mismos (como puede ser el derecho a la intimidad o el derecho a la protección de datos personales). Con ello se quiere poner de manifiesto que el propósito del legislador no ha sido tanto el de reconocer unos <<derechos digitales>> al trabajador, sino el de ofrecer más garantías respecto a las anteriormente existentes frente a las actuaciones que el empleador pueda llevar a cabo, mediante la implantación de dispositivos digitales (y que, en determinadas ocasiones puedan llegar a conculcar derechos o intereses fundamentales).

³⁰ Vid. SSTC 186/2000, de 10 de julio, rec. 2662-1997 y 39/2016, de 3 de marzo, rec. 7222-2013.

³¹ Vid. SSTC 292/2000, de 30 de noviembre rec. 1463-2000 y 29/2013, de 11 de febrero, rec. 10522-2009.

³² Vid. los artículos 79-97 comprendidos en el “Título X Garantía de los derechos digitales” de la LODD.

Centrándonos ahora en los arts. 87 y 89 de la LODD, el art. 87 se conecta directamente con el derecho a la intimidad pues ofrece a los trabajadores una garantía de protección frente a la facultad del empleador de controlar el cumplimiento de las obligaciones laborales³³. El objetivo del precepto es establecer que la única finalidad para la que se prevé la utilización de estos sistemas por parte de la empresa es la de *“controlar el cumplimiento de las obligaciones laborales o estatutarias”*. Se pretende garantizar un uso razonable de este tipo de sistemas digitales, y para ello se impone una serie de exigencias a quién puede hacer uso de los mismos.

Se dispone así, que la empresa deberá *“establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado”*.

Los límites respecto al uso y el acceso a los dispositivos digitales que se permite al trabajador deben ser, pues, conocidos por éste. La redacción de esta nueva Ley es clara: el empleador debe informar al trabajador acerca de cuál es el uso privado de los dispositivos que se tolera al trabajador.

Por su parte, el artículo 89 del citado cuerpo legal regula el tratamiento de las imágenes obtenidas por la empresa del trabajador, una regulación que está innegablemente conectada también con el derecho a la intimidad de todos los trabajadores y con su derecho a que se garantice la protección de sus datos personales. El legislador pretende fijar las condiciones que el empleador debe

³³ Artículo 20.3 ET: *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”*.

cumplir para poder <<tratar>> las imágenes o datos que haya podido obtener de sus trabajadores a través de dispositivos de videovigilancia y de grabación de sonidos en el lugar del trabajo.

Destaca, también que el artículo 89 remite expresamente al contenido de lo dispuesto en el ET, concretamente en el artículo 20.3 que regula el poder organizativo del empleador.

Así, el art. 89 reconoce al empleador la facultad de poder <<tratar>> las imágenes obtenidas a través de sistemas de cámaras o videocámaras siempre que la función de las mismas se limite a controlar a los trabajadores en el ejercicio de sus funciones y siempre y cuando, se respeten también los límites establecidos legalmente. Por tanto, delimita las finalidades para las que el empleador puede justificar la utilización de estos dispositivos de videovigilancia, sin que, en ningún caso, puedan ser utilizados para otras distintas.

En segundo lugar, incide el precepto en la ya mencionada obligación de informar a los trabajadores *“con carácter previo y de forma expresa, clara y concisa”* sobre la medida adoptada en la empresa. Ahora bien, tras imponer dicha obligación con carácter inexcusable, se prevé igualmente una sola excepción en la que no es precisa esta información y es en aquellos supuestos en que *“se haya captado la comisión flagrante de un acto ilícito por los trabajadores”*. Solamente cuando ello ocurra, y para evitar el que pueda descubrirse *“in fraganti”* al presunto infractor, el deber de información se entenderá agotado con la existencia en el lugar de trabajo de un dispositivo informativo en lugar suficientemente visible, dispositivo al que se refiere el artículo 22.4 de la propia LODD³⁴.

³⁴ Artículo 22.4 de la LODD: *“El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.”* En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento”.

En tercer lugar, el segundo apartado del artículo 89 prohíbe taxativamente la utilización de dichos sistemas en determinadas zonas del lugar del trabajo como las zonas dedicadas al descanso o esparcimiento, así como los vestuarios, aseos o comedores. Mediante esta previsión se reserva a los trabajadores determinadas zonas en las que su intimidad y privacidad no va a verse vulnerada bajo ninguna circunstancia ni bajo ningún pretexto. Por ello, en caso de captar imágenes en estas zonas el empleador vulneraría lo aquí dispuesto.

Finalmente, el último apartado del artículo 89º cumple la finalidad de reforzar estas medidas de control empresarial en el lugar mismo del trabajo de manera que se autorizan éstas siempre que *“resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores (...)”*.

Así las cosas, tras haber analizado detalladamente los preceptos más relevantes de la nueva LODD (que tan relevante resulta para el estudio del presente trabajo) podemos concluir que, con carácter general, la mayoría de los preceptos promulgados acerca de la necesidad de garantizar la intimidad de los trabajadores en el ámbito laboral, han reforzado las garantías ya existentes en lo que respecta al derecho a la protección de tales datos personales. Se trata de medidas necesarias en una sociedad como la nuestra, en la que los sistemas y dispositivos digitales están implementándose muy rápido y cobrando mucho protagonismo en el día a día.

5. EL DATO PERSONAL CONVERTIDO EN PRUEBA: VALIDEZ DE LAS IMÁGENES OBTENIDAS A TRAVÉS DE SISTEMAS DE VIDEOVIGILANCIA COMO PRUEBA EN EL PROCESO LABORAL.

5.1 Cuestiones procesales controvertidas en torno a la prueba obtenida a través de cámaras de videovigilancia.

5.1.1 Naturaleza y fuerza probatoria.

En torno a la prueba obtenida mediante sistemas de videovigilancia existen dos cuestiones que en la práctica vienen generando cierta problemática: en primer lugar, nos planteamos si los hechos recogidos mediante cámaras de videovigilancia pueden constituir un medio de prueba válido o no, al haber quedado fijados en soportes o instrumentos de grabación de imagen y sonido (distintos de la tradicional prueba documental). La segunda de ellas, íntimamente ligada a la primera y para el caso de haber sido admitida como prueba válida por el juez de instancia, se refiere a la calificación que debe recibir dicha prueba a los efectos de poder ser o no objeto de recurso extraordinario de suplicación previsto en el artículo 193 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social como ulterior vía de revisión de hechos declarados probados. Al análisis de estas dos cuestiones dedicaremos este epígrafe.

Como adelantábamos, uno de estos problemas reside en la incertidumbre sobre si este tipo de pruebas pueden equipararse a la prueba documental o no. La duda suscitada en torno a dicha cuestión tiene su origen en el hecho de que nuestra Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil nada indica en la regulación destinada a definir la prueba documental sobre si tienen cabida dentro de ésta las pruebas obtenidas por medios de reproducción de imágenes. A ello debemos sumar que la LRJS señala en su artículo 193 que la revisión de hechos probados que pueda efectuarse a través del recurso de suplicación solamente puede llevarse a cabo a través de las pruebas documentales y periciales practicadas. Pues bien, frente a esta normativa nos cuestionamos si cabe la posibilidad en el marco de un recurso de suplicación, de modificar los

hechos probados con base en una prueba videográfica aportada en el juicio, habiendo sido reproducida y constatada su transcripción en fase probatoria. A la vista de que los indicados preceptos no nos dan una respuesta clara al respecto debemos atender a los diversos pronunciamientos judiciales que han abordado la presente cuestión en aras a proporcionar una solución frente a esta laguna normativa.

Si bien tradicionalmente han existido dos tesis o consideraciones altamente contrapuestas sobre la concepción documental de la prueba videográfica³⁵, parece que en la actualidad la doctrina científica se ha posicionado por aquella más restrictiva o literal que considera que por prueba documental no cabe entender la obtenida mediante una grabación realizada con sistemas de videovigilancia y que a su vez se alza frente aquella más extensiva y que años atrás venía admitiendo que la prueba obtenida mediante sistemas de videovigilancia si se asemejaba en cierta medida a la prueba documental recogida en la LEC, por lo que afirmaba que sí podía ser objeto del recurso de suplicación³⁶.

Centrándonos en la que a día de hoy es la posición adoptada por nuestros tribunales – tesis restrictiva o literal – debemos entender que los hechos probados a través de estos medios digitales no podrán ser revisados en virtud del artículo 193 LRJS, al no tener cabida dentro de la conceptualización de <<pruebas documentales>> pues como bien manifiestan los defensores de la misma, la prueba obtenida mediante <<instrumentos de filmación, grabación y semejantes>> tiene entidad propia, lo que la distingue de los documentos

³⁵ Sobre esta cuestión, Vid. TALÉNS VISCONTI, E.E., “Video-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros”, Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, núm. 3, 2018, pp.75 y ss.

³⁶ Esta segunda posición, parte de la consideración de que una grabación de imagen o sonido comparte características básicas con la prueba documental, lo que podría llevar a considerarla dentro del ámbito del recurso de suplicación, pudiendo los hechos probados mediante la misma, ser revisados en sede de suplicación. Para sustentar esta consideración entiende, además, que la prueba obtenida mediante estos sistemas al igual que la prueba documental, puede ser perfectamente revisada por el órgano *ad quem*, a diferencia de otras pruebas como las de interrogatorio de parte o testigos que por el principio de inmediación no pueden ser revisadas por el órgano superior en las mismas condiciones que el órgano *a quo*.

públicos o privados y por ende, lo que hace excluir a la misma de poder ser objeto del recurso de suplicación ex artículo 193 LRJS.

En esta línea se pronuncia la Sentencia del Tribunal Supremo (Social) nº 3983/2010 de 16 de junio de 2011 al entender que la prueba basada en grabación de imágenes que había sido aportada en el acto del juicio no podía ser tratada como prueba documental propiamente dicha y, por ende, no procedía revisar los hechos objeto de grabación. La mentada sentencia zanjó la tradicional problemática sobre esta cuestión, reconociendo la naturaleza autónoma de los medios de reproducción de la palabra, el sonido y la imagen, diferenciándolos definitivamente de la prueba documental³⁷.

Por tanto, esta posición doctrinal - hoy imperante entre nuestros tribunales – entiende que aceptar la entrada de las grabaciones como documentos susceptibles para alegar error por parte del juzgador de instancia, supondría el que éstos fueran valorados de nuevo, sustituyendo la apreciación del juez de instancia por el Tribunal *ad quem*, lo que supondría un quebrantamiento del principio de inmediación de absoluto respeto como principio procesal.

5.1.2 Aportación al proceso laboral.

Antes de profundizar en la presente cuestión, conviene asentar el marco legal relativo a la prueba en el proceso (concretamente en el proceso laboral).

Por un lado, la LRJS dedica sus artículos 90 a 96 a desarrollar las pruebas y medios probatorios. Pues bien, especial atención merece el artículo 90 por cuanto faculta a las partes del proceso para aportar cuantos medios de prueba estimen necesarios, siempre que los mismos se encuentren regulados en la Ley y mediando previa justificación de su utilidad y pertinencia. Dicho precepto

³⁷ Vid. STS (Social) de 16 junio 2011, rec. 3983/2010 en la que se manifiesta que: “*el recurso de suplicación tiene el carácter de extraordinario, tal y como resulta de su configuración legal expresamente reconocida en su propia regulación (...). Dicho carácter, asimismo, ha sido reconocido por el Tribunal Supremo y por el Tribunal Constitucional. Consecuencia de tal carácter es la limitada revisión de hechos legalmente permitida, que únicamente puede realizarse a la vista de la prueba documental o pericial practicada en la instancia, por lo que la interpretación del concepto de prueba documental, a la vista del carácter del recurso, necesariamente ha de ser efectuada de forma restrictiva*”.

deja claro que también podrán aportarse al proceso *“los de reproducción de la palabra, imagen y sonido”*.

Por su parte, la LEC, anticipa en su artículo 299 que se admitirán como medios de prueba *“los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso”*, para posteriormente en su artículo 382, dejar claro que serán admisibles en el proceso, los medios de prueba de *“reproducción de imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes”*.

Dicho lo cual, podemos afirmar que nuestra normativa prevé la posibilidad de que las imágenes obtenidas a través de sistemas de videovigilancia sean aportadas al proceso como medio de prueba válido.

Dejando a un lado las distintas tesis que se manifiestan sobre la naturaleza de este tipo concreto de prueba (y que ya hemos tenido ocasión de analizar), conviene ahora centrarnos en el carácter que cabe otorgar a las mismas cuando su obtención ha supuesto la vulneración de algún derecho fundamental (en particular, la intimidad o la protección de datos).

Nuestra doctrina jurisprudencial es unánime en considerar que cuando para la obtención de este tipo de pruebas se han conculcado derechos fundamentales, la prueba deviene nula. Hasta aquí parece que en la práctica no suelen aparecer grandes conflictos.

Tampoco parecen suscitarse grandes problemas cuando al acto del juicio se aportan junto a estas pruebas videográficas (nulas) otras de distinta naturaleza - tales como pruebas testificales - que confirman los hechos recogidos en las imágenes obtenidas por los sistemas de videovigilancia y que no hacen más que respaldar la pretensión de quién aporta la prueba videográfica (el empleador), pues los Tribunales vienen considerando el despido como procedente (art. 55.4 ET) aún cuando al acto del juicio se haya aportado una

prueba videográfica vulneradora de derechos fundamentales, pues el motivo del despido no se fundamenta evidentemente en ella, sino en otra u otras de distinta naturaleza que confirman la conducta inadecuada del trabajador merecedora de la medida empresarial. Es decir, que cuando la prueba videográfica (a pesar de haber conculcado derechos fundamentales) se apoye en una o varias pruebas que de manera suficiente acrediten la conducta objeto del despido, el mismo deberá ser calificado como procedente por haberse acreditado suficientemente la conducta denunciada en virtud de estas otras (y siempre dejando bien claro que la decisión del Tribunal no se apoya en la prueba videográfica vulneradora de derechos, sino en las otras que con absoluto respeto a los derechos del trabajador, confirman la conducta merecedora del despido). En ese sentido se ha pronunciado la STSJ (Social) de Pamplona nº 52/2019 de 18 de febrero³⁸, resolución que resulta de gran importancia por ser uno de los primeros pronunciamientos que abordan esta cuestión tras la aparición de la nueva LODD. Se resuelve por el Tribunal un caso de despido disciplinario en el que, como prueba para acreditar la conducta llevada a cabo por uno de los trabajadores y merecedora de despido disciplinario, la empresa aporta unas imágenes captadas a través de las cámaras de videovigilancia instaladas en el centro de trabajo. El Tribunal, tras hacer un extenso y detallado análisis de la reciente normativa en materia de protección de datos y en especial, del artículo 89 de la citada Ley, y teniendo en cuenta todas las circunstancias concretas del caso, estima que el tratamiento realizado por la empresa de las imágenes obtenidas a través de los sistemas de videovigilancia implantado en la empresa era ilícito por lo que la prueba consistente en dichas grabaciones debe ser considerada nula y por ende, excluida del proceso. No obstante y, pese a ello, el Tribunal declara la procedencia³⁹ del despido, aunque apoyando el fallo en la comprobación de los hechos por la aportación al proceso de pruebas testificales, concretamente la de dos testigos que de manera clara revelaron las circunstancias en las que se

³⁸ Rec. 875/2018.

³⁹ Vid. STSJ (Social) de Pamplona nº 52/2019 de 18 de febrero, rec. 875/2018: *“El que se haya inadmitido la prueba de la grabación de las cámaras de seguridad no quiere decir que en el presente caso los hechos que se imputaban al demandante en la carta de despido no hayan quedado acreditados con otros medios probatorios que no estén vinculados o relacionados con lo captado en las cámaras de videovigilancia”*.

produjo la agresión del demandante y del otro trabajador, viéndose implicados en una pelea que, finalmente, determinó el despido disciplinario de los dos trabajadores.

Ahora bien, cuando junto a este tipo de pruebas no se aportan al proceso otras de distinta naturaleza que puedan confirmar la conducta objeto del despido, la pregunta es: ¿cuál es entonces la postura adoptada por nuestros tribunales, la de considerar el despido nulo o improcedente?

En este sentido no encontramos una línea argumentativa asentada que camine hacia la misma dirección ya que algunos pronunciamientos consideran que cuando la pretensión del empleador de despedir a un trabajador se apoya única y exclusivamente en una prueba videográfica obtenida ilícitamente (por vulnerar derechos fundamentales), el despido debe ser reputado nulo (artículo 55.5 del ET)⁴⁰. Así lo entendieron las sentencias de SSTJ (Social) del País Vasco nº609/2013, de 9 de abril⁴¹ y nº470/2018, de 27 de febrero⁴², fallando que la sanción laboral impuesta usando como medio de prueba un video obtenido ilícitamente deviene nula y por ende, el despido también al haberse obtenido vulnerando derechos fundamentales.

Y sin embargo, otros pronunciamientos sostienen que el despido debe ser considerado improcedente⁴³ (y no nulo), pues entienden que la nulidad de la prueba no provoca directamente la nulidad del despido, sino más bien su improcedencia por ausencia de causa, al no existir otras pruebas que prueben la conducta ilícita atribuida al trabajador. Así lo han fallado sentencias como la STSJ (Social) de Madrid, nº691/2019 de 10 de julio⁴⁴ que en el mismo sentido

⁴⁰ Art. 55.5 ET: *“será nulo el despido que tenga por móvil alguna de las causas de discriminación prohibidas en la Constitución o en la ley, o bien se produzca con violación de derechos fundamentales y libertades públicas del trabajador”*.

⁴¹ Rec. 445/2013.

⁴² Rec. 226/2018.

⁴³ Produciendo tal decisión los efectos previstos en el artículo 56 ET para el caso de declararse el despido improcedente.

⁴⁴ Rec.440/2019.

consideró que el despido era improcedente pues la empleadora aportó, como única prueba para justificar el despido, las grabaciones de dos cámaras ocultas obtenidas indebidamente. Por tanto, al no existir otras pruebas que verificasen la conducta objeto del despido, el mismo debería considerarse improcedente. También otras como la STSJ (Social) de Castilla-La Mancha nº25 /2018, de 12 enero⁴⁵ o la STSJ (Social) de Cataluña, nº 4224/2018 de 12 de julio⁴⁶ .

Llegados a este punto, podemos comprobar la importancia que tiene el hecho de que los medios de grabación de imágenes se utilicen conforme a la Ley, pues como puede apreciarse, su uso incorrecto acaba por hacer ineficaz en sede judicial cualquier grabación llevada a cabo por la empresa con fines de fiscalización laboral. No cabe duda alguna de que en nuestro sistema de derecho, cualquier prueba obtenida con vulneración de derechos fundamentales conduce a la expulsión de ésta del proceso, cualquiera que sea su naturaleza u origen, lo que en ningún caso significa que las pruebas basadas en imágenes y sonidos deban ser rechazadas siempre y en todo caso, pues siempre que su uso respete los derechos consagrados en nuestra Constitución, se admitirá como cualquier otro medio de prueba válido previsto en nuestra legislación.

⁴⁵ Rec.1416/2017.

⁴⁶ Rec. 2803/2018.

6. CONCLUSIONES

- PRIMERA. Las nuevas tecnologías se han convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Su llegada ha supuesto para todo ciudadano el reconocimiento de oportunidades pero también grandes riesgos relacionados con el derecho individual a la privacidad.
- SEGUNDA. Resulta innegable que la digitalización experimentada por nuestra sociedad también ha alcanzado al ámbito laboral. La rapidez con la que avanza la tecnología en este contexto hace necesaria una normativa que esté a la altura de las nuevas situaciones en las que los trabajadores pueden ver debilitados sus derechos fundamentales.
- TERCERA. La ausencia de una regulación específica sobre esta materia ha llevado a nuestros Tribunales a realizar una importante labor interpretativa dirigida a resolver las controversias suscitadas en la práctica.
- CUARTA. La búsqueda de un equilibrio entre los intereses y bienes constitucionales que esta materia tiende a confrontar es, sin duda, la tarea más compleja a la que se enfrenta nuestro legislador.
- QUINTA. El derecho a la protección de datos ha ido adquiriendo protagonismo con el paso del tiempo, llegando a configurarse como un verdadero y autónomo derecho fundamental, diferenciándose paulatinamente del tradicional derecho a la intimidad.
- SEXTA. La legislación española en materia de protección de datos ha procurado siempre caminar en el mismo sentido que el resto de los países de la Unión Europea, prueba de ello es la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que entre sus finalidades

contempla la de instaurar un sistema de derechos digitales cada vez más uniforme y garantista.

- SÉPTIMA. No obstante lo anterior, la velocidad con la que avanza la tecnología es siempre mayor a la de nuestra normativa por lo que las dudas existentes en torno a esta cuestión siguen inundando la mayoría de las empresas españolas que siguen cuestionándose cómo deben emplear estos medios de videovigilancia de manera lícita.
- OCTAVA. Tanto el legislador como nuestros Tribunales deberán seguir esforzándose en delimitar todavía más esta materia evitando en la medida de lo posible la inseguridad jurídica a la que nos hemos tenido que enfrentar durante todos estos años.
- NOVENA. La validez de la prueba obtenida por medios de grabación videográfica es esencial de cara a la posibilidad de poder usar ésta como mecanismo que sirva para probar la ejecución de actos ilícitos que puedan derivar en la imposición de sanciones disciplinarias o, incluso, en un despido procedente. Por eso es esencial que las empresas conozcan qué instrumentos pueden utilizarse para que puedan desenmascarar conductas ilícitas de los empleados cuando éstas se produzcan, sin afectar ni atentar ello a los derechos fundamentales de los trabajadores implicados.
- DÉCIMA. Al respecto ha sido clave la doctrina judicial que ha entendido en qué casos pueden las empresas poner cámaras para grabar a los trabajadores, y que estas grabaciones puedan alegarse como prueba válida - documental - en primera instancia, y también si cabe a revisión de estas pruebas videográficas en el recurso de suplicación.

BIBLIOGRAFIA

- AA.VV. (MONEREO PÉREZ, J.L. Dir.), "Manual de Derecho Procesal Laboral: Teoría y práctica", Madrid, Tecnos, 2014, 3ª ed., pp. 292-306.
- ALEMÁN CANO, J., "Temas teórico-prácticos del proceso laboral" Albacete, Bormazo, 2012, 1ª ed., pp. 66-73.
- ARIAS DOMINGUEZ A. y RUBIO SÁNCHEZ F., "El derecho de los trabajadores a la intimidad", Pamplona, Thomson Aranzadi, 2006, 1ª ed., pp. 169-177.
- FERNÁNDEZ DOCAMPO, M.B. "La eficacia revisora de los medios de reproducción de la palabra, la imagen y el sonido en el recurso de suplicación", Revista Doctrinal Aranzadi Social, nº 13, 2003, pp. 4-13.
- GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I.A, "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", Revista Española de Derecho del Trabajo, nº 216, 2019, pp. 12 - 27.
- GARCÍA SALAS, A.I, "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018", Revista de Información Laboral, nº 2, 2018, pp. 2-4.
- GONZÁLEZ GONZÁLEZ C., "Control empresarial de la actividad laboral mediante la videovigilancia y colisión de los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", Revista Aranzadi Digital, nº 1, 2018, pp. 1-18.
- MARTÍNEZ GIRON, J.; ARUFE VARELA, A. y CARRIL VÁZQUEZ, X.M, "Derecho del trabajo", A Coruña, Netbiblo, 2004, 1ª. ed., pp. 249-260.

- ORTEGA GIMÉNEZ, A., "Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de datos de la UE", Revista Española de Derecho del Trabajo, nº 216, 2019, pp. 2-4, 6, 9, 26, 27.
- SERRANO OLIVARES, R., "Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", Revista luslabor, 3º, 2018, pp. 222-225.
- TALÉNS VISCONTI, E.E., "Video-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, núm. 3, 2018, pp. 59-77.
- TOSCANI GIMÉNEZ D. y VALENCIANO SAL A., "Derechos fundamentales inespecíficos de los trabajadores", Albacete, Bormazo, 2016, 1ª ed., pp.125-138.

LEGISLACIÓN

- Constitución Española de 1978 («BOE» núm. 311, de 29/12/1978).
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras («BOE» núm. 296, de 12/12/2006).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal («BOE» núm. 298, de 14 de diciembre de 1999).
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil («BOE» núm. 7, de 08/01/2000).
- Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social («BOE» núm. 245, de 11/10/2011).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales («BOE» núm. 294, de 6 de diciembre de 2018).
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores («BOE» núm. 255, de 24/10/2015).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) («DOUE» núm. 119, de 4 de mayo de 2016).

ANEXO JURISPRUDENCIAL

La jurisprudencia consultada y estudiada para la realización del presente trabajo comprende el conglomerado de sentencias que aparecen a continuación:

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

STEDH de 9 de enero 2018 (Asunto López Ribalta y otros contra España).

Tras detectarse en un supermercado diferencias entre el inventario de productos y lo facturado en las cajas, se decide instalar cámaras de videovigilancia (unas visibles y otras ocultas). Tras un tiempo en funcionamiento, las mismas revelan cómo algunos de los empleados se encuentran implicados en robos ocurridos en el propio supermercado (en algunas ocasiones llevados a cabo por ellos mismos y en otras, facilitándose su realización por algunos clientes). Los propios trabajadores reconocen estar involucrados en los hechos grabados por las cámaras, por lo que la empresa procede a despedirlos. Los trabajadores objeto del despido disciplinario impugnan el mismo ante la jurisdicción social por entender que la instalación de las cámaras ocultas reveladoras de su conducta han vulnerado su derecho fundamental a la protección de datos. La pretensión de los trabajadores es desestimada tanto por el Juzgado de lo Social como por el TSJ, entendiendo ambos que la videovigilancia encubierta llevada cabo por la empresa sin haber comunicado previamente a los trabajadores su instalación, es procedente y conforme al artículo 20 ET, precepto que permite la utilización de medidas de control y vigilancia siempre que se cumpla el test de proporcionalidad, triple juicio que entienden superado en el caso en cuestión. El asunto llegó ante el TEDH, por entender que se había vulnerado el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en su artículo 8. El Tribunal de Estrasburgo recuerda que los datos visuales obtenidos a través de cámaras de videovigilancia suponen el almacenamiento y procesamiento de datos de carácter personal, estrechamente vinculados a la esfera privada de las personas, razón ésta por la que los trabajadores deben ser informados previamente, de modo expreso, preciso e inequívoco. Además

índice en que los trabajadores tienen una expectativa razonable de respeto a su privacidad y que la empresa no cumple con los requisitos exigidos legal y jurisprudencialmente. Por ello, el TEDH concluye que no hay un justo equilibrio entre el derecho de las demandantes al respeto de su vida privada y el interés del empresario en la protección de sus derechos propietarios, y que la actuación empresarial vulnera el citado art. 8 del Convenio.

TRIBUNAL CONSTITUCIONAL

- STC 98/2000, de 10 de abril (Asunto Casino de la Toja), rec. 4015/1996, ECLI:ES:TC:2000:98.

El origen de este asunto proviene de la instalación en el Casino de La Toja de unos micrófonos que permiten recoger y grabar las conversaciones que pueden producirse en las secciones de caja y de la ruleta francesa. Uno de los trabajadores en nombre del Comité de Empresa del Casino de La Toja S.A., invoca el derecho a la intimidad ante el juez de lo Social al considerar que al no haber mediado comunicación al Comité de Empresa, tal instalación atenta contra el derecho a la intimidad de los trabajadores del casino, habida cuenta de que éste ya dispone de un circuito cerrado de televisión que funciona correctamente. La pretensión del trabajador es estimada por lo que se ordena el cese inmediato de dicha iniciativa empresarial. Por el contrario, el TSJ parte de una tesis distinta, sosteniendo que el centro de trabajo no es un lugar donde el trabajador haga empleo de su derecho a la intimidad, y justificando las medidas tomadas por la empresa porque suponen un <<plus de seguridad>> añadido al sistema ya presente en el centro de trabajo. En síntesis, según este Tribunal, la empresa está totalmente capacitada para conocer el contenido de las conversaciones de los trabajadores, tanto de éstos entre sí como con los clientes. El asunto es recurrido en casación ante el TC, órgano que defiende que en el centro de trabajo sí se ejerce el derecho a la intimidad razón por la que la celebración del contrato de trabajo no puede implicar en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano, por más que el ejercicio de tales derechos en el seno de la organización productiva pueda admitir ciertas

modulaciones o restricciones. El TC razona que la mera utilidad o conveniencia para la empresa *“no legitima la instalación de tales aparatos, que suponen una intromisión ilegítima en la intimidad, al permitir captar comentarios privados, tanto de los clientes como de los trabajadores del casino”*.

- **STC 186/2000, de 10 de julio (Asunto Ensidesa), rec. 2662/1997, ECLI:ES:TC:2000:186.**

El asunto versa sobre el despido de un cajero del economato de ENSIDESA tras ser sorprendido sustrayendo dinero en repetidas ocasiones por unas videocámaras que enfocan la caja registradora y el mostrador de paso. La empresa que sospecha sobre la conducta indebida del trabajador debido a unos desajustes contables que se han producido en la sección donde éste presta sus servicios, decide tomar la decisión de instalar las cámaras de videovigilancia no informando al Comité de empresa. El trabajador presenta una demanda en el Juzgado de lo Social instando su improcedencia, entendiendo que las pruebas en las que se fundamenta su despido se obtienen vulnerando sus derechos fundamentales, demanda que concluye con una sentencia en la que se califica el despido como procedente, al entender el juzgador que la medida empresarial está plenamente justificada y es idónea para la consecución del objetivo que persigue, que no es indagar sobre la vida privada del cajero sino comprobar cuál es el verdadero comportamiento laboral del trabajador, y, por lo tanto, admite como prueba del despido la grabación de las cintas donde aparece el actor. Esta sentencia es recurrida en suplicación en el TSJ, órgano que desestima el recurso al considerar que las filmaciones no van referidas a la vida íntima del trabajador. De nuevo, esta sentencia del TSJ es recurrida ante el Tribunal Supremo, por medio de un recurso de casación para la unificación de doctrina que, finalmente, es inadmitido.

- **STC 292/2000, de 30 de noviembre, res. 1463/2000, ECLI:ES:TC:2000:292.**

Este asunto es promovido por el Defensor del Pueblo, respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El Tribunal Constitucional establece el derecho a la protección de datos como derecho fundamental autónomo, derecho que

implica para todo ciudadano disponer de un conjunto de facultades consistentes en obtener información sobre el destino o uso de los datos y de acceder a los mismos, rectificarlos y cancelarlos. El objeto de protección del derecho fundamental a la protección de datos, según el TC, no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que ya está protegido por el artículo 18.1 de la CE, sino los datos de carácter personal. En efecto, cualquier limitación que el ordenamiento jurídico imponga a tales facultades ha de venir amparada en el mandato de una norma con rango de ley.

- **STC 29/2013, de 12 de marzo (Asunto Universidad de Sevilla), rec. 10522/2009, ECLI:ES:TC:2013:29.**

El supuesto enjuiciado en este pronunciamiento trata sobre un trabajador de la Universidad de Sevilla al que se ha sancionado disciplinariamente por infracciones referidas al cumplimiento de su horario laboral, al constatarse de tales ilícitos a partir de las imágenes grabadas por las cámaras de videovigilancia instaladas en el recinto universitario (vestíbulo y zonas de paso público), respecto a las que cuenta con autorización administrativa de la AEPD para, entre otros fines, el control de acceso de las personas de la comunidad universitaria. En dicho recinto existen distintivos anunciando la presencia de las cámaras y la captación de imágenes, si bien, no se informa al trabajador de que las grabaciones pueden utilizarse para supervisar el cumplimiento de sus obligaciones contractuales. El TC recuerda la doctrina establecida sobre este precepto constitucional en la STC 292/2000, de 30 de noviembre y con apoyo en ella afirma que las imágenes grabadas constituyen un dato de carácter personal protegido por la Constitución en su art.18.4 por permitir la identificación de la persona, que tal exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles, límites que sólo la ley puede fijar y que en ningún caso basta como fundamento el interés empresarial de controlar la actividad laboral ni tampoco que ese tratamiento de datos resulte eventualmente proporcionado al fin

perseguido. Añade que es necesaria una información <<previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida>> y que <<debe concretar las características y el alcance del tratamiento de datos que va a realizarse, esto es, en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que pueden utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo>>. En consecuencia, siendo este el criterio, la Sentencia considera que, en el caso, para entender cumplida la exigencia de información no basta ni la presencia de distintivos en el recinto universitario que anuncien la instalación de las cámaras, ni tampoco que la creación del fichero se haya notificado a la AEPD, por lo que la conducta de la Universidad de emplear las grabaciones de imagen para controlar el cumplimiento del contrato por parte del trabajador, sin haber informado a éste sobre esa utilidad de supervisión laboral, resulta contraria al mentado precepto constitucional, sin ser necesario si quiera examinar el tratamiento de los datos personales desde el enfoque de la proporcionalidad.

- STC 39/2016, de 3 de marzo (Asunto Bershka), rec. 7222/2013, ECLI:ES:TC:2016:39.

El supuesto examinado tiene origen en el despido de una trabajadora por apropiarse de dinero en la caja del comercio en que la que presta sus servicios, conducta esta que se constata mediante grabaciones de la cámara de videovigilancia que la empresa ha ordenado instalar como consecuencia de la previa detección de irregularidades en dicha caja, sin ser comunicada a los trabajadores, pero sí colocándose en el escaparate del establecimiento, en lugar visible, el distintivo informativo de que el centro está videovigilado. Con relación a estos hechos, el TC valora si la decisión judicial de dar validez a esta prueba es contraria a los artículos 18.1 y 18.4 de la CE, resolviendo que en el caso enjuiciado no hay vulneración del artículo 18.4 CE porque la trabajadora puede conocer, mediante el correspondiente distintivo colocado en el escaparate de la tienda donde trabaja, la existencia de las cámaras y la finalidad para la que han sido instaladas. Por otra parte, tampoco aprecia la

vulneración del artículo 18.1 CE, que igualmente invoca la recurrente en amparo, porque considera que la medida de instalación de cámaras de seguridad para el control de la zona de caja es, de acuerdo con la doctrina de la STC 186/2000 de 10 julio, una medida justificada, idónea, necesaria y equilibrada.

TRIBUNAL SUPREMO

- STS (Social) de 16 de junio de 2011, rec. 3983/2010 (RJ/2011/7266), ECLI:ES:TS:2011:6216.

Tras haber demandado el trabajador a la empresa en la que trabaja por producirse una disputa entre éste y otro compañero suyo (el actor alega ser discriminado por parte de éste en diversas ocasiones, razón por la que presenta denuncia en reclamación de tutela de la libertad sindical y derechos fundamentales), pretensión que resulta desestimada por entender que no procede revisar el relato de hechos probados de la sentencia de instancia. El juzgador deniega dicha revisión argumentando en la sentencia que no se trata de una prueba documental o pericial propiamente dicha, por lo que su revisión debe ser rechazada. La sentencia es recurrida en casación, siendo de nuevo desestimado el recurso. El recurrente aporta una sentencia de contraste en la que sí se admite la prueba de cintas videográficas como documental a efectos revisorios. Existiendo un claro contraste entre ambas sentencias, el recurso es admitido a trámite. La sentencia en cuestión trata de dilucidar si las grabaciones de audio y vídeo, aportadas al acto del juicio tienen o no el carácter de prueba documental a efectos de la revisión de los hechos declarados probados al amparo del art. 191 b) LPL. Tras un pormenorizado análisis sobre la mentada cuestión, el TC rechaza el recurso planteado por el trabajador al considerar que la grabación de audio y vídeo no tiene naturaleza de prueba documental, a efectos de fundar una revisión de hechos probados ex art. 191 LPL.

TRIBUNAL SUPERIOR DE JUSTICIA

- STSJ (Social) de País Vasco nº 609/2013 de 9 abril, rec. 445/2013 (AS/2014/1362), ECLI:ES:TSJPV:2013:2441.

El asunto versa sobre el despido de una trabajadora que realiza las funciones de cajera en un supermercado. Las cámaras de videovigilancia instaladas en el centro de trabajo graban a la misma evitando el escaneo de diversos productos en beneficio de su pareja, motivo éste por el que la empresa procede a su despido disciplinario por transgresión de la buena fe contractual. Las referidas cámaras son instaladas en 2008 sin especificar en el momento de su colocación que se trata de un sistema de videovigilancia laboral, al contrario, se plantea como un sistema destinado a evitar robos por terceros, advirtiéndose incluso que algunas de las cámaras no van a estar operativas (sin indicarse cuáles si y cuáles no). La trabajadora interpone demanda solicitando que se declare nulo el despido por realizar la empresa un uso ilegítimo de las grabaciones recogidas por las cámaras al no haberle informado de manera previa, clara y precisa sobre la finalidad e instalación, considerando vulnerado su derecho a la intimidad, pretensión que fue estimada. El supermercado interpone recurso de suplicación solicitando la declaración procedente del despido, sin embargo el Juzgado de lo Social mantiene la nulidad del despido al considerar que la prueba videográfica en la que se basa la empresa para probar en juicio los hechos imputados en la carta de despido es nula, por atentar al derecho a la intimidad de la trabajadora al no comunicarle a los trabajadores la existencia del sistema de vigilancia con carácter previo a su instalación. Asimismo, añade el Juzgador que los medios probatorios consistentes en grabación de imágenes aportados por la empresa no pueden ser considerados prueba documental y por ende, tampoco medios aptos para la reforma fáctica por vía de suplicación laboral. Por tanto, basando la empresa su despido única y exclusivamente en las pruebas videográficas aportadas al juicio, y siendo estas nulas por vulnerar el derecho a la intimidad de la trabajadora al no respetar su instalación los requisitos exigidos por la jurisprudencia, el recurso debe desestimarse, debiendo confirmarse la sentencia que declara nulo el despido.

- STSJ (Social) Castilla-La Mancha nº25/2018, de 12 enero, rec. 1416/2017, (AS/2018/566), ECLI:ES:TSJCLM:2018:1.

El asunto trata sobre el despido de un trabajador que desarrolla la función de vigilante de seguridad y que tras haber sido amonestado verbalmente por fumar dentro de las instalaciones de la fábrica donde desempeña sus funciones (a sabiendas de que está prohibido fumar en el recinto ya que existen carteles en los que se indica que <<se prohíbe fumar>>), continúa haciéndolo. Junto a dicha conducta, se le imputa una disminución voluntaria y continuada en su puesto de trabajo así como otros actos inmorales llevados a cabo por el trabajador, motivos por los que la empresa precede a su despido. La empresa tiene conocimiento de dichas actuaciones al haber instalado una cámara de grabación en el interior de la caseta donde éste trabaja pero sin avisarle con carácter previo de la instalación, pues la finalidad de la empresa no es otra que la de comprobar la sospecha de que fuma en dicho lugar (existen avisos y advertencias de la existencia de cámaras de videovigilancia en el interior del recinto empresarial, pero no en el interior de la caseta). Frente a la decisión de despido, el trabajador interpone demanda solicitando la nulidad del despido, resultando la misma desestimada al considerar el Juzgador que el despido es procedente pues considera suficientemente probada la conducta indebida del trabajador generadora del despido tanto por las grabaciones obtenidas como por las declaraciones de varios testigos que corroboran la misma. El trabajador recurre en suplicación solicitando la revisión de hechos probados y la declaración de nulidad de su despido por vulneración de derechos fundamentales (derecho a la intimidad). La sentencia resuelve el primer motivo recordando que es doctrina asentada del TS que el carácter extraordinario del recurso de suplicación impide a las partes no sólo alegar o probar hechos nuevos sino también modificar los hechos declarados probados por el Juez *a quo*, lo que deriva del hecho de que hay una sola instancia, y por consiguiente, el único juez competente para valorar en su plenitud la prueba es el que celebra el juicio. El segundo motivo que lleva a declarar el despido improcedente revocando la sentencia en cuestión se argumenta con apoyo en la STC 39/2016, de 3 de marzo de 2016, considerando que el hecho de que el actor no sea informado previamente por la empresa de su intención de instalar

una cámara de videovigilancia en la caseta en la que presta sus servicios ante la sospecha de que está cometiendo irregularidades laborales no vulnera, en principio, el derecho del trabajador a la protección de la intimidad. No obstante, en apoyo a la citada sentencia, considera que el comportamiento empresarial descrito no cumple el triple julio de proporcionalidad exigible a toda medida restrictiva de derechos fundamentales ya que aunque existan sospechas de que el trabajador fuma estando prohibido (idónea), no puede afirmarse que la medida sea necesaria, al existir otros medios más moderados y menos agresivos del derecho a la intimidad personal del trabajador (como por ejemplo el testimonio de los compañeros o la prueba de la contratación de una empresa de desinfección para higienizar la caseta), medios suficientes con los que la empresa puede acreditar el pretendido incumplimiento.

- STSJ (Social) Pamplona nº 52/2019 de 18 de febrero, rec. 875/2018 (AS/2019/1014), ECLI:ES:JSO:2019:281.

El asunto versa sobre el despido de un trabajador por participar en una pelea con otro trabajador de la empresa, conducta que es acreditada a través de las cámaras de videovigilancia instaladas en el lugar donde ocurrieron los hechos así como por las declaraciones testificales de otros trabajadores, testigos presenciales de los hechos. El trabajador demanda a la empresa, entre otros motivos, por considerar que las grabaciones obtenidas por el sistema de videovigilancia vulneran su derecho a la intimidad y a la protección de datos personales por no cumplir con los requisitos exigidos por la normativa y jurisprudencia de aplicación (principalmente, deber de información previa). El Juzgador entiende que debe inadmitirse la prueba consistente en el visionado de las grabaciones realizadas por las cámaras de seguridad puesto que la empresa no cumple con las exigencias vinculadas al necesario respeto al derecho de protección de datos que ampara al trabajador, incluyendo el deber informativo sobre la existencia de sistema de videovigilancia y la propia finalidad para la que se utiliza, incluyendo la posibilidad de sancionar si captan actos ilícitos o incumplimientos laborales. Ahora bien, pese a considerar nula la prueba basada en grabación de imágenes, procede a declarar procedente el despido con fundamento en la valoración de otras pruebas que permiten

acreditar el incumplimiento laboral imputado al trabajador (declaraciones de testigos que presenciaron los hechos y que confirman la realidad de los hechos de la conducta imputada a la trabajadora).

- STSJ (Social) de País Vasco nº470/2018, de 27 febrero, rec. 226/2018 (AS/2018/1200), ECLI:ES:TSJPV:2018:557.

El supuesto versa sobre el despido de una trabajadora, decisión extintiva que toma la empresa tras haber constatado a través de las cámaras de videovigilancia instaladas en el supermercado donde ésta trabaja, que la trabajadora realiza manipulaciones fraudulentas en el cobro de artículos de caja (tales como la de anular tiques), actuaciones que suponen un grave perjuicio para la empresa ya que además los clientes se llevan los artículos de la tienda sin que el importe de la compra sea ingresado en la caja por la actora, de forma que también se le imputa una apropiación fraudulenta de cierta cantidad de dinero. La cámara que capta la actuación indebida de la trabajadora es instalada encima de su caja como medida justificada, equilibrada y razonada, debido a sospechas razonables de la comisión de irregularidades en ese punto de venta. La trabajadora interpone demanda solicitando la declaración de nulidad de su despido por vulneración de derechos fundamentales, pretensión que es estimada por el Juzgador. Frente a dicha resolución, el supermercado interpone recurso de suplicación que es desestimado, por lo que se confirma la sentencia que declara el despido nulo y ello porque la instalación de las cámaras de videovigilancia reveladoras de los hechos generadores del despido suponen un incumplimiento por parte de la empresa del deber de información al trabajador sobre la existencia de dicho sistema de videovigilancia, sobre el fichero y sobre el tratamiento de los datos de carácter personal, su finalidad y destino de la información. A ello cabe añadir, que en el caso enjuiciado no se aporta ninguna otra prueba, al margen de las grabaciones controvertidas, de que la actora cometa los hechos imputados generadores del despido.

- STSJ (Social) de Cataluña, núm 2803/2018 de 12 de julio, rec. 2803/2018 (JUR/2018/281030), ECLI:ES:TSJCAT:2018:6381.

El asunto versa sobre un trabajador que es despedido por realizar trabajos por su cuenta no facturados a la empresa utilizando las instalaciones, maquinaria y materias primas de ésta, actuación que se acredita a través de las cámaras de videovigilancia instaladas en la empresa donde éste trabaja, instalación que se lleva a cabo sin comunicación previa al trabajador con el único objetivo de averiguar si éste lleva a cabo tales trabajos de manera oculta. Las cámaras revelan cómo el trabajador sí las realiza por lo que la empresa toma la decisión de despedirle. El trabajador interpone Papeleta de Conciliación sobre el despido disciplinario improcedente contra la empresa, que resulta sin aveniencia. Contra dicha sentencia la empresa anuncia recurso de suplicación, considerando que el uso de sistemas de videovigilancia no exige ni el consentimiento ni el conocimiento del afectado para su tratamiento (apoyándose en la STC 186/2000, de 10 de julio), considerando que basta con que la medida supere el triple juicio de proporcionalidad (idoneidad, necesidad y proporcionalidad), requisitos que, según ésta, se cumplen en el caso enjuiciado. El juzgador desestima el recurso al entender que el hecho de que no se informe al trabajador sobre la instalación de las cámaras de grabación violenta sus derechos o libertades fundamentales, por lo que no puede tener ningún efecto, y por ende, los hechos imputados en la carta de despido no se pueden considerar probados.

- STSJ (Social) de Madrid nº 691/2019 de 10 julio, rec. 440/2019 (JUR/2019/249494), ECLI:ES:TSJM:2019:5351.

El asunto versa sobre el despido disciplinario de un trabajador que presta los servicios de camarero en una empresa, la cual le notifica la carta de despido disciplinario por sustraer diariamente unas determinadas cantidades de dinero de la caja registradora así como productos o incluso, por no cobrar o a clientes sus consumiciones. La empresa conoce de dichas actuaciones gracias a las imágenes grabadas por las cámaras de videovigilancia instaladas de manera oculta en la cafetería en la que éste trabaja. El trabajador demanda a la empresa por considerar el despido improcedente, pretensión que es estimada

por el Juzgador. Frente a dicha sentencia, la empresa interpone recurso de suplicación, el cual es desestimado al considerar que las pruebas basadas en imágenes han sido obtenidas de manera ilícita, motivo por el que deben considerarse nulas. Siendo que las grabaciones de la dos cámaras ocultas son la única prueba aportada por la empresa demandada para justificar su decisión y que estas son nulas, debe confirmarse la sentencia que declara el despido improcedente y ello porque corresponde la carga de la prueba a la empresa de probar la veracidad de los hechos imputados en la carta de despido, hechos que no han quedado acreditados, deviniendo la decisión extintiva empresarial improcedente.